Listing of Claims:

1. (Canceled).

2. (Currently Amended) ~~The~~ A cryptographic ~~anonymous signature~~ method ~~according to claim 1~~[[,]] of anonymously signing a message by a member of a group comprising a plurality of members each equipped with calculation means and associated storage means, the method initially comprising:

a first step of calculating, at first calculation means of a trusted authority, a pair of asymmetric keys common to the members of the group and comprising a common public key and a common private key;

a second step of calculating, at the first calculation means of the trusted authority, a group public key associated with the members of the group;

a third step of calculating, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key for each member of the group and storing the private key in the storage means of the each member, each group private key being associated with the group public key and being different for each member of the group;

a fourth step of determining, at the first calculation means of the trusted authority, as many symmetrical secret keys as there are members of the group; and

a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to

obtain as many encrypted forms of the common private key as there are non-revoked members;

on each revocation of a member from the group, the method further comprising:

a sixth step of modifying, at the first calculation means of the trusted authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key;

a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members; and

when a non-revoked group member anonymously signs a message to be sent to an addressee, the method further comprising:

an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member;

a ninth step of calculating, at the calculation means of the signing member, an anonymous signature of the message using the group private key for the signing member; and

a tenth step of calculating, at the calculation means of the signing member, an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing

member;

wherein the group is constituted at a date t1 and the method further comprises:

during the first step associating, at the first calculation means, the common private key with an updated date equal to t1; and

during the third step storing, at the storage means of each member, the updated date of the common private key;

wherein at the time of each revocation within the group at a date t2:

during the sixth step modifying, at the first calculation means of the trusted authority, the updated date to determine an updated date equal to the date t2; and

wherein on each anonymous signing by the member of the group of the message to be sent to the addressee:

during the eighth step, the common private key stored in the storage means of the signing member is updated only if the updated date in the storage means of the signing member is also different from the updated date of the up-to-date common private key updated by the first calculation mean.

3. (Currently Amended) ~~The~~ A cryptographic ~~anonymous signature~~ method ~~according to claim 1~~[[,]] of anonymously signing a message by a member of a group comprising a plurality of members each equipped with calculation means and associated storage means, the method initially comprising:

a first step of calculating, at first calculation means of a trusted authority, a

pair of asymmetric keys common to the members of the group and comprising a common public key and a common private key;

a second step of calculating, at the first calculation means of the trusted authority, a group public key associated with the members of the group;

a third step of calculating, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key for each member of the group and storing the private key in the storage means of the each member, each group private key being associated with the group public key and being different for each member of the group;

a fourth step of determining, at the first calculation means of the trusted authority, as many symmetrical secret keys as there are members of the group; and

a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the common private key as there are non-revoked members;

on each revocation of a member from the group, the method further comprising:

a sixth step of modifying, at the first calculation means of the trusted authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key;

a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret

keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members; and

when a non-revoked group member anonymously signs a message to be sent to an addressee, the method further comprising:

an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member;

a ninth step of calculating, at the calculation means of the signing member, an anonymous signature of the message using the group private key for the signing member; and

a tenth step of calculating, at the calculation means of the signing member, an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member;

wherein the method further comprising:

during the third step calculating, at the first calculation means, an identifier of the member for each member of the group and storing the identifier of the each member of the group in the storage means of each member; and

calculating, at the first calculation means of the trusted authority an identifier for each new member of the group on each revocation within the group.

4. (Currently Amended) The cryptographic method according to claim 3, further ~~omprising~~ comprising:

during the third step storing, at storage means connected to the first calculation means of the trusted authority, the symmetrical secret key of each member, the group public key, the public key common to the members of the group, each of the encrypted forms of the common private key, and each of the identifiers, each encrypted form of the common private key being associated with one of the identifiers; and

for each modification of the composition of the group that corresponds to a revocation of one of the members of the group, the method further comprising:

removing the secret key of that member from the storage means connected to the first calculation means of the trusted authority; and

to update the common private key stored in the storage means of the member, the method further comprising:

reading, at the calculation means of the member, the encrypted form of the common private key stored in the storage means connected to the first calculation means of the trusted authority and associated with the identifier of the member; and

decrypting, at the calculation means of the member, the encrypted form of the common private key previously read using the secret key stored in the storage means of the member.

5. (Currently Amended) ~~The~~ A cryptographic method ~~according to claim 1~~[[,]] of anonymously signing a message by a member of a group comprising a plurality of members each equipped with calculation means and associated storage means, the method initially comprising:

a first step of calculating, at first calculation means of a trusted authority, a pair of asymmetric keys common to the members of the group and comprising a common public key and a common private key;

a second step of calculating, at the first calculation means of the trusted authority, a group public key associated with the members of the group;

a third step of calculating, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key for each member of the group and storing the private key in the storage means of the each member, each group private key being associated with the group public key and being different for each member of the group;

a fourth step of determining, at the first calculation means of the trusted authority, as many symmetrical secret keys as there are members of the group; and

a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the common private key as there are non-revoked members;

on each revocation of a member from the group, the method further comprising:

a sixth step of modifying, at the first calculation means of the trusted

authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key;

a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members; and

when a non-revoked group member anonymously signs a message to be sent to an addressee, the method further comprising:

an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member;

a ninth step of calculating, at the calculation means of the signing member, an anonymous signature of the message using the group private key for the signing member; and

a tenth step of calculating, at the calculation means of the signing member, an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member;

wherein the ~~further~~ method further comprising:

during the third step storing, at storage means connected to the first calculation means of the trusted authority, the secret key of each member, the pair of asymmetric keys common to the members of the group, and the group public

key; and

on each modification of the composition of the group that corresponds to a revocation within the group:

eliminating the secret key of a revoked member from the storage means connected to the first calculation means of the trusted authority; and

to update the common private key in the storage means of the member, the method further comprising:

reading, at the calculation means of the member the encrypted forms of the common private key in the storage means connected to the first calculation means of the trusted authority; and

using, at the calculation means of the member, the secret key in the storage means of the member to decrypt the encrypted forms of the common private key.

6. - 11. (Canceled)